

Public Hearing Testimony, CT State Education Committee
Raised Bill No. 7017-An Act Concerning Student Data Privacy
March 19, 2015

Senator Slossberg, Representative Fleischmann and Members of the Education Committee,

My name is Dr. Kimberly Norton and I am here to testify today on Raised Bill No. 7017.

The State of Connecticut is in good company with the proposal of Raised Bill 7017, An Act Concerning Student Data Privacy. In 2014, 36 out of 46 states with legislative sessions introduced student data privacy bills. Twenty states passed 28 student data privacy bills into law. I would like to commend you for beginning to tackle this issue by Raising Bill 7017.

Public education has changed dramatically with the advent of technology. There is so much data being collected on our children through their use of online services, apps, and websites, as well as through the development of extensive State Wide Longitudinal Data Systems, that parents are confused and have been left out of the discussion, especially with 2011 changes to the Family Educational Rights and Privacy Act (FERPA).

Parental consent is now a thing of the past. Not only do parents not know what sites, apps or online platforms their kids are using, they don't know who has access to their child's data, how it is being used and how it will be used in the future. Combine advances in technology with significant FERPA changes not requiring parental consent to access student records, and the floodgates are open for all kinds of issues to arise regarding student privacy.

For Connecticut parents, Raised Bill 7017 starts the important work of protecting children's educational records and privacy. While I think it a good start, I would like to recommend that this bill be amended to exclude any allowable data collection that is not in the sole interest of the education of children. Being pro-business is great for businesses but children should not be required to participate in online activity that enhances the profit of private companies. So by allowing private companies to use kids' data for product development, enhancement and marketing doesn't seem like a good idea. In addition, allowing companies holding very profitable established databases to merge, purchase, or acquire companies without written consent of families is not a good idea either.

Furthermore, the bill also makes reference to "current industry standards" and holding private companies to these standards. However, these standards are a work in progress and cannot be counted on to protect children's data, which is why 20 other states have passed 28 student data privacy bills in 2014. Let's define those standards and be explicit.

Sec. 3 allows local and regional boards to disclose directory information to "any person requesting it" for a good reason. This provision is too broad and needs to be more explicit or deleted altogether.

In addition to data collected by online companies, which is the focus of Raised Bill 7017, districts collect data as well, which include student responses to standardized assessments. Bill 7017 specifically excludes student assessment data from its protections. It needs to be included in the definition of "student generated content", as does sensitive survey data that is collected by districts. District collected data used to be kept in file cabinets. Now with a click, it can be forwarded out of district, out of state, and to other authorized representatives without parental

permission due to changes in FERPA. Parents need to be informed that FERPA has changed and allows for nonconsensual disclosure of their child's education data. The old adage, "no news is good news", is not the case when it comes to sharing of children's educational records. Parents need to know.

Children's school records, which includes their academic performance, behavioral observations, psychological data, assessment data and potentially 300 plus other data points, as recommended by the National Education Data Model for longitudinal database development, need to be protected by law.

Just as you have done with online vendors, contractors and operators, the state needs to have a serious discussion to limit data mining and sharing of student data within government entities and those authorized representatives doing research for them.